

Drive apparatus for safety-critical components, and a corresponding method

The present invention relates to a drive apparatus for open-loop or closed-loop control of a safety-critical component having a switching device which has a first switch and a second switch, which is connected in series with the first, for switching the safety-critical component, a first control device for reception of an input signal and emission of a first drive signal, and a second control device for reception of the input signal and for emission of a second drive signal. The present invention also relates to a corresponding method for open-loop or closed-loop control of a safety-critical component.

Many safety applications require a very short reaction time for processing of an EMERGENCY-OFF demand. Although present-day modern safety appliances generally use microcontrollers and internal functions can therefore be processed very quickly, filter algorithms have to be used, because of burst and RF interference, in order to achieve the maximum availability. Further boundary effects such as compensation for the cable capacity and dynamic input testing in the end lead to relatively long evaluation times.

A further problem is represented by the fact that, in safety appliances from Category SIL3 with respect to the European IEC Standard 615 08, two controllers must always be used for hardware redundancy and fault tolerance reasons.

The applicant has solved this problem, in the case of safety appliances, by using two controllers with identical hardware and

identical firmware for safety appliances. A "master/slave principle" is used in order to make it possible to identify systematic faults. This means that one of the controllers is in each case the master for a short time, while the other is the slave. The two controllers interchange this status after a defined time. One of the controllers is normally used to drive specific switches, for example in a load circuit on an electrical machine while, in contrast, the other controller is used to monitor the switching states of these switches, and itself drives other switches of other components.

That controller which is in the master mode reads all of the inputs and defines the output states of the switches to which it is connected or which are allocated to it. Important states such as demands are matched with the slave, and internal tests are carried out.

An EMERGENCY-OFF demand is first of all registered by the controller in the master mode. One disadvantage in this case is that those outputs which are driven by the controller in the slave mode cannot be switched off until the EMERGENCY-OFF demand has been transmitted from the master to the slave. Those outputs which are driven directly by the master can be switched off relatively quickly. The reaction time for switching off the driven components is thus dependent on which controller receives the demand first of all, and whether the desired output can also be switched off by this controller.

Demand times of less than 45 milliseconds have not been possible to achieve until now with the described circuit design. Correspondingly faster hardware would allow the demand time to be reduced down to 35 milliseconds. However, this is not sufficient for critical demands such as press controls.

The object of the present invention is thus to propose a drive apparatus and a corresponding method for open-loop or closed-loop control of a safety-critical component, whose reaction time is shortened on average.

According to the invention, this object is achieved by a drive apparatus for open-loop or closed-loop control of a safety-critical component having a switching device which has a first switch and a second switch, which is connected in series with the first, for switching the safety-critical component, a first control device for reception of an input signal and emission of a first drive signal, and a second control device for reception of the input signal and for emission of a second drive signal, wherein the first switch in the switching device can be driven by the first control device and the second switch in the switching device can be driven by the second control device.

The invention also provides a method for open-loop or closed-loop control of a safety-critical component by provision of a switching device which has a first switch and a second switch, which is connected in series with the first, for switching the safety-critical component, provision of a first control device, which is connected to the switch, and of a second control device which is connected to the second switch, reception of an input signal and emission of a first drive signal from the first control device to the first switch in the switching device on the basis of the input signal, wherein the second control device emits a second drive signal to the second switch in the switching device on the basis of the input signal.

The invention is based on the idea that the output should be switched off irrespective of which of the

switches is turned off first all. Since both controllers or control devices now drive the series circuit comprising the two switches and this results in the outputs of the controllers being AND-linked, the output to the switching device is switched off in all cases with the shorter reaction time of the two controllers.

One positive side-effect of this time-offset switching is that simultaneous welding of the two switches, for example contactors, can be precluded. The EMERGENCY-OFF function is thus still ensured even after welding of one of the contacts of the switches.

The time-offset switching-off of the switches also has the advantage that approximately the same life can be expected of both switches. This is because each switch is switched off with equal frequency, statistically on average, with and without current flowing through it.

The first and the second switch in the switching device are preferably each formed by a relay or a contactor. Alternatively, the first and the second switch may, however, also be in the form of semiconductor switches or may comprise an optocoupler.

The first and the second switch may be driven with a time offset with respect to one another. Furthermore, the first and the second control device may operate on the master/slave principle, thus resulting in a defined time offset. The time offset is then, specifically, governed by the time period which the master requires in order to make the slave aware of an event.

An electrical machine with a load circuit is advantageously equipped with the said drive apparatus according to the invention. In this case, the drive apparatus may

be used in particular for safety disconnection or EMERGENCY-OFF control.

The present invention will now be explained in more detail with reference to the attached drawings, in which:

Figure 1 shows a circuit diagram of a drive apparatus according to the invention; and

Figure 2 shows a time signal diagram of the drive apparatus shown in Figure 1.

The exemplary embodiments described in the following text represent preferred embodiments of the present invention. Two contactors S1 and S2 are used in the circuit diagram shown in Figure 1 and are connected in series with one another in order to switch a load circuit, which is not illustrated, of an electrical machine via the terminals K1 and K2. Two control devices or controllers C1 and C2 are used to drive the two contactors S1 and S2. The output signals from the controllers C1 and C2 are converted by the respective output units Y1 and Y2 into corresponding movements of the contactors S1 and S2. The two controllers C1 and C2 receive their input signal from an input unit X which, for example, may be in the form of an EMERGENCY-OFF switch. This input signal is checked by respective clock signals T1 and T2 at the input X of the controllers C1 and C2.

Figure 2 shows a signal waveform diagram or state diagram of the individual components for this purpose. The EMERGENCY-OFF switch at the input X is pressed at the time t0. The controller C1 reads the input X at this time. After a certain reaction time, the output unit Y1 is switched off at the time t1. Since the controller C2 was not active at the time t0, it must first of all be informed by the controller C1 that the EMERGENCY-OFF

switch has been pressed, in order to switch off the output unit Y2. The reaction time is thus

correspondingly longer, and the output unit Y2 is not switched off until the time t2.

In one specific embodiment, the drive apparatus according to the invention may be used in a safety appliance, for example the 3TK2845 model series from the applicant, with two floating relay outputs, which are connected in series. The reaction time of the master to an EMERGENCY-OFF demand is typically up to 8 milliseconds. The time to transmit the EMERGENCY-OFF demand from the master to the slave may be up to 15 milliseconds. In the present example, the maximum tripping time for the relay is 12 milliseconds. With the standard circuitry according to the prior art, in which relays connected in series are driven only with the aid of one controller the reaction time would be up to $8\text{ ms} + 15\text{ ms} + 12\text{ ms} = 35\text{ ms}$. With the circuitry according to the invention, with a so-called "cascaded output", the reaction time would be at most $8\text{ ms} + 12\text{ ms} = 20\text{ ms}$ since each controller C1, C2 switches one of the relays or one of the contactors S1, S2 so that there is no longer any need to transmit the EMERGENCY-OFF demand to the slave in order to switch off the load circuit. The demands are thus satisfied even for very time-critical applications. The relays or contactors S1, S2, which are connected in the form of a logic AND link, in the switching device when driven according to the invention can still make use of the appliances which have been used in the past without any need for changes in the hardware or firmware for a safety disconnection.